Australian Government
Department of Finance

May 2026

Embracing the potential of verifiable credentials in the Commonwealth

Consultation paper – Part A

Table of Contents

1. Privacy collection notice **3**

2. Introduction **4**

3. What we are consulting on **5**

3.1 Developing Commonwealth VC policy settings 5

3.2 Consultation purpose 5

3.3 Providing feedback 5

4. Navigating this consultation process **6**

5. A Commonwealth VC Trust Framework **7**

5.1 Scope and purpose of the framework 7

5.2 The framework as guidance 7

5.3 Alignment with national strategy 8

5.4 International examples 8

6. Key issues and considerations **9**

6.1 VCs may enhance efficiency and grow productivity 9

6.2 Finding the right use cases that will benefit from VCs 10

6.3 Interoperability is the key to broad adoption 11

6.4 There is not yet an agreed best-practice for VCs 11

6.5 Ensuring a trustworthy VC system 12

6.6 Providing strong safeguards 13

6.7 Understanding how VCs can promote inclusion 13

6.8 Adopting VCs may create unexpected risks 14

7. Our questions for you **15**

Appendix A – Key concepts for VCs **16**

Participants in a VC system 16

Lifecycle of a VC 17

Appendix B – Glossary **18**

1. Privacy collection notice

Your personal information is protected by law, including the *Privacy Act 1988*, and is collected by the Department of Finance (Finance) to manage the submissions provided as part of its consultation on the Australian Government's proposed policies for verifiable credentials. The personal information collected in this public consultation may be disclosed to Finance employees, other Australian Government agency employees, as well as relevant State and Territory Government officials, where appropriate or necessary to report on feedback, and formulate policy and related recommendations to Government on verifiable credentials.

Please do not provide any personal or sensitive information relating to another person, unless you have sought that person's consent to provide their information for this purpose and have shown them this Privacy Collection Notice. Additionally, we ask that responses do not include any unnecessary personal or sensitive information, and note if it is provided, it will be collected.

Submissions may be released and made publicly available on the Digital ID System website. Submitters may, as part of the submission process indicate that they would like their submission, or part of their submission to remain confidential.

Additionally, Finance may disclose your submission(s) to third party service providers and third-party service provider artificial intelligence software to assist and inform analysis of submissions. Third parties who contract with Finance are contractually bound to protect personal information in accordance with the Privacy Act. Finance will not use or disclose the personal information collected in this consultation for another purpose without your consent unless required or authorised by law.

For more information about how Finance handles your personal information, including information about access to or correction of your personal information, please visit our Privacy Policy at: https://www.finance.gov.au/publications/policy/department-finance-privacy-policy.

2. Introduction

Every day we need to prove facts about ourselves as we go about our lives. We might be asked to verify our identity for a bank account, prove we're over 18 to enter licensed premises, show that we hold essential qualifications for a profession, or demonstrate we have a permit or licence to work a shift in a specific occupation or industry.

Historically we use physical credentials to prove these facts, such as plastic cards we carry with us, or official documents that we file and retrieve when needed. Common examples include driver licences, passports, proof of age/photo ID cards, trade qualifications or security passes to access a place of work.

All of these are taken as authoritative proof of relevant attributes about people, businesses, and other organisations that entities can confirm – and others in the community rely upon – so that we can participate in everyday life. Collectively these are called 'credentials'.

Many credentials are provided by Australian governments at all levels. A wide range of credentials are also provided and relied upon by the private sector.

Accessing credentials can be time-consuming and may require queuing in-person during business hours, filling in paper forms and waiting for a credential to arrive in the post. The increasing use of online services is also transforming the way we want and need to use our credentials.

A relatively new technology known as 'verifiable credentials' (VCs) has emerged. VCs provide a digital alternative to physical credentials, overcoming the need for credentials to be issued and held in physical form only. Instead, they can be issued digitally in near real-time, securely stored on your phone or other device, and carried with you to be used where and when you need them. VCs may also prove useful to underpin other new technologies, for example agentic AI.

Importantly, while VCs provide a digital alternative to traditional credentials, physical versions can still be used by those who prefer or need them.

However, the technology is only part of the picture. For VCs to be used safely and effectively in Australia, the right balance of policy and regulatory settings needs to be achieved, as well as determining what, if any, legislative change is required.

As the VC system continues to evolve, the Australian Government (the Government) is seeking views from the community on its proposed VC policies and any issues or opportunities to be considered in the next stage of policy development.

Two separate, though connected, papers have been prepared:

- Part A: *Embracing the potential of verifiable credentials in the Commonwealth* (this document) is the primary consultation paper and addresses high-level considerations relevant to VCs.
- Part B*: Proposed Commonwealth policy positions for the use of verifiable credentials*, contains 9 modules that present a range of proposed policy positions for VCs that are being considered by Government.

This approach is intended to assist you to easily identify the areas of the consultation you would like to engage with and to provide targeted comments and feedback.

3. What we are consulting on

3.1 Developing Commonwealth VC policy settings

The VC landscape, both locally and internationally is rapidly evolving. The Government has a role to play in the VC system, particularly to help build trust within that system. This consultation provides a channel for the community to provide feedback on proposed VC policy settings and the potential development of a Commonwealth VC Trust Framework.

The policies and trust framework will be primarily developed to guide Commonwealth agencies adopting VCs, as both issuers of Commonwealth VCs and verifiers of VCs. The framework may also offer useful guidance for jurisdictions and organisations outside the Commonwealth that may choose to adopt aspects of it when implementing VCs.

The Government considers that the development of VC policies and an associated framework will play a part in creating the common foundations for interoperability, accessibility and consumer protection across the VC system, and will also promote opportunities for innovation and productivity growth.

3.2 Consultation purpose

This public consultation provides the opportunity to collect and consider your feedback through written submissions and further build on the work undertaken to date by the Government. The purpose of this consultation is to:

- Share insight and generate public discussion about the relevant issues related to the Commonwealth's role in the VC system.
- Allow the Government to consider views from the public, including Australian businesses and other organisations, to inform policy development.
- Surface issues and opportunities to be considered as part of determining the Government's VC policy settings and scope of the trust framework.
- Inform further VC policy development to enhance public trust and confidence in VCs.

3.3 Providing feedback

The consultation period will open on Wednesday 20 May 2026 and close at 11:59pm AEST Friday 3 July 2026. Details on how to provide your feedback are available on the Have Your Say page on the Digital ID System website.

Consultation timeline

Key steps	Timeframe
Public consultation ***opens***	**Wednesday 20 May 2026**
Public consultation ***closes***	**11:59pm AEST Friday 3 July 2026**

4. Navigating this consultation process

To support you in responding to this consultation process we have prepared two separate, though connected, consultation papers. This approach recognises the breadth of subject matter that needs to be considered and organises content to make it easier for stakeholders to provide feedback.

- Part A: *Embracing the potential of verifiable credentials in the Commonwealth* (this document) is the primary consultation paper that presents a high-level overview of the broader opportunities, challenges, and potential risks for VCs.
- Part B: *Proposed Commonwealth policy positions for the use of verifiable credentials* is organised into 9 modules that present a range of proposed policy positions for VCs being considered by the Government. Part B provides stakeholders with a deeper interest in the details of VC policy and invites views on specific proposed policy positions.

This approach is intended to help you to easily identify areas of the consultation you would like to engage with and provide targeted comments and feedback across one or both papers. All feedback provided is welcome and will be considered by the Government.

The modules described in Part B are:

- Selection of Commonwealth use cases
- Issuers
- Verifiers
- Digital wallets
- Commonwealth trust services
- Privacy and consumer protection
- Voluntariness and inclusion
- Interoperability and standards
- Security.

5. A Commonwealth VC Trust Framework

5.1 Scope and purpose of the framework

VCs will only be useful if people want to use them. People will be more likely to use VCs if they are safe, secure, easy to use, give them a tangible benefit, and preserve their privacy.

The two primary objectives of a Commonwealth VC Trust Framework would include:

- facilitating interoperable VCs to drive greater efficiency in how credentials are used across the economy, thereby improving productivity over time, and
- ensuring that the people, businesses, and other organisations using VCs are properly protected.

The trust framework would also provide guidance to implementers of VCs to help them make sure that the VCs they issue and rely on are useful.

A trust framework aims to provide a system that is interoperable and secure, while allowing users to safely and securely share information and attributes about themselves or the entities they represent. Trust frameworks bring together tailored policy, technical settings, and may potentially incorporate specific regulations to establish standardised processes and practices.

Taken together, the components of a Commonwealth VC Trust Framework aim to address some of the challenges that must be overcome in a VC system, including:

- Implementing VCs so that they are interoperable and can be presented and verified at any time and place, to increase productivity and efficiency and drive down costs for people, businesses, and other organisations.
- Ensuring VCs are issued to the right person or organisation.
- Government, businesses, and other organisations can rely on digital verification technology to give confidence that VCs have not been altered and are legitimate.
- Providers of VC services are trustworthy and proactively protect the users of their systems and the data they handle.

5.2 The framework as guidance

The Government's current predisposition is that the Commonwealth VC Trust Framework will initially be implemented as a guidance-based policy instrument, rather than through one or more regulatory alternatives. As Commonwealth policy, the framework would shape the decisions and delivery of VCs by Commonwealth agencies, while ensuring sufficient flexibility is retained so that the framework could be voluntarily adopted – in part or in whole – by other organisations.

Importantly, VCs are a relatively new and emerging technology. Significant evolution and change are likely to come in the near to medium term before best practices (including in relation to technology) are established.

The introduction of a Commonwealth VC Trust Framework as a guidance-based policy instrument does not preclude the incorporation of regulatory mechanisms at a later date. For instance, regulation may be required should future decisions of Government seek to strengthen the governance of one or more aspects of VC policy.

5.3 Alignment with national strategy

The Commonwealth VC Trust Framework would be established in alignment with the *Digital ID and Verifiable Credentials Strategy*[1], which was developed jointly by the Commonwealth, State and Territory governments. The *Digital ID and Verifiable Credentials Strategy* sets out the nationally agreed direction and priorities for Digital ID and VCs in Australia.

A Commonwealth VC Trust Framework would provide guidance for Commonwealth agencies to help them to deliver against this strategy, in particular to support realisation of Outcome 3 'Creating the framework for delivering interoperable credentials'.

5.4 International examples

The Government understands that similar frameworks are being considered or actively developed in internationally, for example in the EU and NZ.

Europe's Electronic Identification, Authentication, and Trust Services (eIDAS) aims to ensure secure digital transactions across the EU internal market by establishing common rules for electronic identification and trust services.[2]

Similarly, New Zealand's *Digital Identity Services Trust Framework Act 2023*[3] introduces a number of legislative provisions related to VCs, as well as providing for the creation of more detailed rules.[4]

[1] Digital ID and Verifiable Credentials Strategy
[2] eIDAS Regulation
[3] *Digital Identity Services Trust Framework Act 2023*
[4] *Digital Identity Services Trust Framework Rules 2024*

6. Key issues and considerations

The Government is seeking your feedback on issues that it should consider in developing a Commonwealth VC Trust Framework. The sub-sections below invite you to provide responses to several known policy issues, though these are not intended to be exhaustive. We invite you to raise any additional issues in your feedback that you consider relevant.

Further detail on these and other issues is provided in Part B: *Proposed Commonwealth policy positions for the use of verifiable credentials*.

6.1 VCs may enhance efficiency and grow productivity

Early feedback has indicated that VCs may have the potential to increase the efficiency with which credentials are used in Australia and, accordingly, help to grow productivity across the economy. These views recognise the opportunities that may be created by design features inherent to VCs, such as user control, selective disclosure, and data minimisation.

Potential productivity enhancing effects of VC include, but are not limited to:

- Reducing regulatory and compliance burden, as well as lowering barriers to accessing services, with standardised and automated credential verification processes that are reusable across multiple sectors.
- Reducing fraud by making it easier for government and businesses to detect illegitimate credentials and to stop attempted fraud at the source (particularly identity fraud).
- Reducing the economic impact of data breaches by incorporating data minimisation by design, constraining the amount of data that needs to be shared, and driving down the prevalence with which copies of physical credentials are stored across the economy.
- Increasing labour availability and streamlining employee onboarding, with easily shareable and verifiable skill profiles.
- Increasing the speed of access to finance by overcoming document verification challenges between customers and financial institutions.
- Increasing access to foreign markets through supply chain VCs that provide assurance to businesses and governments of the origin and regulatory compliance of traded goods.
- Opening the door to innovation and new, more efficient, business models that utilise the beneficial features of VCs, such as AI Agents.

These potential efficiency and productivity enhancements need to be understood in the context of what they might mean on a day-to-day basis for the people, businesses, and other organisations that may use VCs. This will be informed by a range of factors, for example the magnitude of productivity gain, how much demand there is for adoption of VCs, and the ability to achieve these productivity gains at scale and across sectors.

A key focus area of this consultation is to understand the extent to which VCs can enhance economic efficiency and help to grow productivity in Australia.

6.2 Finding the right use cases that will benefit from VCs

VCs that are aligned with emerging international standards have the potential to reshape the way Australians access and use their credentials.

These benefits may include:

- Making the issuing and presentation of credentials more secure and trustworthy through the use of modern technologies (e.g. robust cryptography).
- Streamlining processes for issuing, reissuing, updating, and revoking credentials if they are lost, or expired.
- Supporting vulnerable people during natural disasters or in a crisis situation so they can access the support services they need in a timely and efficient way (e.g. Government support payments).
- Enhancing privacy by minimising the need to share and store personal data which can help to mitigate the consequences of data breaches.
- Enabling easier and more convenient user experiences.
- Assuring businesses that the credentials people present to them are current and genuine, helping them to detect and prevent fraud.

Potential benefits will only be realised through the implementation and adoption of VC use cases. While VCs are still in the relatively early stages of adoption domestically and internationally, the Commonwealth, states and territories have worked together to agree the initial set of credentials that should be implemented as nationally interoperable VCs, including driver licences and proof of age cards. Each jurisdiction will determine when it will develop the ability to issue and/or receive nationally interoperable VCs, in accordance with the agreed standards.

From the Commonwealth's perspective it is unclear how much demand is broadly present in the Australian community for the shift from traditional forms of credentials to VCs. This includes understanding which specific Commonwealth credentials might be of most value to the community to warrant investment, and whether the potential benefits are sufficiently compelling to motivate people to make the shift to VCs.

The Government is interested in hearing views on how VCs might be used across the economy and the benefits that may be realised. This relates not only to the issuance of VCs – where government, businesses, and other organisations change their processes to offer VCs alongside existing options for physical credentials – but equally (perhaps more so) what appetite there may be for the acceptance and reliance upon VCs across the economy.

The Government invites views on how you would use VCs, whether as issuer, verifier, or both, and what scale of change and investment you think would be needed to achieve adoption.

The Government is also seeking views on whether agencies, businesses, organisations and individuals would be willing to make the changes and investments needed for VCs to be widely adopted in Australia.

6.3 Interoperability is the key to broad adoption

An overarching objective for a Commonwealth VC Trust Framework for VCs and digital wallets is to facilitate and promote interoperability of VCs domestically and internationally.

Interoperability means that a user can access and store VCs on a device of their choosing, and that they can provide those credentials to any organisation where and when they choose.

Interoperability is not just a technology consideration, it can also be enabled through policy settings such as encouraging voluntary adoption of common standards. Interoperability is relevant for both face-to-face and online use cases, as well as for use cases that extend beyond simple interactions by individuals (such as complex, multi-hop and multi-party use cases involving non-individual entities).

Technical interoperability for VCs means that systems, organisations and jurisdictions can recognise, exchange, and accept the presentation of credentials seamlessly regardless of the issuing platform, whilst maintaining security, trust and privacy. Technical interoperability across participants requires the use of common standards.

The full benefits of VCs can only be realised if broad interoperability is achieved across jurisdictions – domestically and, potentially, internationally. If policy settings do not adequately promote interoperability, some benefits of VCs may still be realised, however they are likely to be localised and constrained by organisational and jurisdictional boundaries. Similarly, regulation (if introduced in the future) that is not technology agnostic can present barriers to supporting the interoperability of VC domestically and abroad.

The Government is interested in understanding whether the high priority currently being placed on interoperability is appropriate, or whether alternative approaches may be considered in the adoption of VCs.

6.4 There is not yet an agreed best-practice for VCs

There is no single, settled, best-practice approach for the technical implementation of VCs, with multiple competing approaches and technical solutions available in the market. Having multiple options leads to the risk that early implementations of VCs will follow different technical designs and will not readily be compatible with other VC solutions. Achieving broad interoperability will be challenging and a lack of interoperable approaches in Australia also has the potential to increase the economic costs of VCs in the economy.

Despite this, there appears to be general recognition across government and industry that a small set of international standards are emerging as the leading options for developing and implementing VCs in Australia and overseas.

The leading options for international standards are understood currently to come from:

- The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC),
- The World Wide Web Consortium (W3C), and
- JSON Web Tokens (JWT) and Selective Disclosure JWT (SD-JWT).

The Government is considering how best to navigate this complexity. As a first step, governments have agreed to support the development of several key VCs across the Commonwealth, states, and territories.

Specifically, through the Data and Digital Ministers Meeting (DDMM) the Commonwealth, state, and territory governments have agreed the initial set of nationally interoperable VCs, which include driver licences and proof of age cards. To achieve national interoperability the Commonwealth, state, and territory governments have agreed to follow the relevant ISO/IEC standards approach where appropriate for implementing these VCs.

The Government recognises that while decisions have been made to support interoperability on an initial set of national VCs, future participation in the VC system will require further implementation considerations for a broader range of Commonwealth VCs.

The Government's current predisposition is that Commonwealth agencies should adopt recognised international VC standards and should not invest in bespoke solutions.

Additionally, rather than dictating a rigid choice of a single technical standard for all use cases, agencies should select the most appropriate international standard that best fits their requirements, noting that the various standards options have different strengths.

The trust framework is expected to incorporate nationally agreed policy settings on VCs and will seek to provide its users with guidance for navigating the complexities of a multi-standards environment.

The Government invites views on the suitability of this strategy and how well it will support the goal of achieving interoperability of VCs in Australia and internationally.

6.5 Ensuring a trustworthy VC system

The technical development of VCs designed and bult in accordance with recognised international standards must include strong protections for users. Importantly, holders must have control over their data at all times and their credentials cannot be shared without their consent. However, as with all digital technology, there is a risk that malicious parties may look for ways to overcome security protections.

The trust framework will seek to address the question of how participants in a VC system: issuers, verifiers, wallet providers, trust service providers (see Appendix A, which defines the roles of participants) – as well as the intermediaries who may be acting on their behalf – should conduct themselves to build and maintain the community's trust in a broader VC system.

The proposed trust framework is expected to include guidance for each of the key participants on expectations of appropriate behaviour. This guidance will stem from key proposed Commonwealth policy positions that are being tested in Part B: *Proposed Commonwealth policy positions for the use of verifiable credentials*.

The Government invites views on behaviours – positive or otherwise – that may present specific opportunities to the Commonwealth, or specific risks/challenges and that may need to be guarded against in a broader VC system.

6.6 Providing strong safeguards

The Commonwealth VC Trust Framework is expected to include guidance aimed at ensuring that the people, businesses, and other organisations that use VCs are adequately protected.

VCs are designed with a number of privacy and security enhancing features including sharing data only with the consent of the individual, and allowing only the necessary data to be shared (which can also be derived from, or a subset of, the source credential).

How effectively these benefits are realised depends on the particular implementation of the VC and the digital wallet that stores it, as well as broader policy and regulatory frameworks that are in place.

The Government's current approach is that existing relevant legislative and regulatory protections on privacy and consumer protection will apply to the trust framework, rather than attempting to introduce new alternatives. General privacy protections for Australians have been in place for many years, notably through the *Privacy Act 1988* and equivalent legislation in the states and territories. Similarly, governments and standards-making bodies have established security frameworks and guidance for the protection of people and businesses using digital systems.

The framework might include additional guidance that helps to protect people using VCs, including to ensure that VCs are only ever issued to the correct person, that digital wallet providers respect the privacy of individuals placing VCs inside them, and that verifiers request only necessary data while also ensuring the ongoing security and privacy of data received through a VC presented to them.

The Government is aware that limitations and trade-offs will be encountered when relying on existing, general, legislation and regulation to protect users of VCs, and invites views on how such an approach may work in practice as part of a guidance-based framework.

6.7 Understanding how VCs can promote inclusion

It is important that VCs are accessible by all Australians and that users have choice to adopt VCs or continue using traditional credentials.

While the impacts that VCs may have on inclusion and accessibility are still being explored, some features of VCs may offer opportunities to advance the inclusivity of digital services provided to people. For example, having access to digitally available VCs can reduce the need for physical copies, which may be of great help to people who experience difficulty in dealing with paper documents. Similarly, the use of a digital wallet as the container for a VC opens opportunities for innovative and inclusive software for people who require additional support.

On the other hand, VCs may not be able to solve all inclusion and accessibility challenges. The benefits of VCs might be difficult to access for people who aren't eligible or cannot prove entitlement to the base credential. Using VCs is also generally dependent upon owning and/or getting private access to a smart device.

Feedback received to date suggests that VCs can enhance the inclusiveness of services. The Government seeks to understand whether this aligns with expectations, and whether stakeholders have additional perspectives on the accessibility and inclusivity of VCs in Australia.

6.8 Adopting VCs may create unexpected risks

The emergence of VC technology brings with it opportunities to improve the lives of Australians. Understandably these opportunities and potential benefits are often the focus of discussions relating to VCs.

However, there are potential downsides, risks, and unintended consequences that may arise from the implementation and adoption of VCs.

VCs rely heavily on technical design elements to preserve privacy and protect people's sensitive data. Bad actors may find ways past these protections through either technical or non-technical means – for example, power imbalances in social/economic interactions could enable the exploitation of selective disclosure to extract excessive data from holders of VCs.

Another key issue is that while current technical protections may be strong and suitable, it's unlikely they always will be. VC design will need to anticipate and keep ahead of new and emerging threats. Other risks could also emerge as part of the transition period as VCs gradually become used in the community.

The Government would like to understand any new or emerging risks that may be introduced to Australia with the adoption of VCs and welcomes views on how such risks should be mitigated in the trust framework. These need not be limited only to risks of the technology, including exposure to cyber security incidents and post-quantum risks, but could be across any aspect of VC adoption such as policy and regulation. New threat vectors for long-standing risks should also be included and considered (for example, fraud, privacy and inclusion).

7. Our questions for you

a. How might the adoption of VCs enhance economic efficiency and help to grow productivity in Australia? How are these effects distinguishable from other ways of accessing and using credentials?

b. What use cases for the adoption of VCs do you think are viable in Australia (from the perspective of both the issuer and the verifier)? Which of these do you think are the most valuable and/or important for the Commonwealth to explore?

c. Are you or your organisation using, or likely to make use of, VCs? If so, how, and what role(s) would you be performing in a VC system?

d. What is the nature and scale of investment that you think is needed to adopt VCs?

e. Are there any barriers preventing Australians from making greater use of VCs – either as holders, verifiers, or as issuers?

f. What matters should a Commonwealth Trust Framework that prioritises interoperability and consumer protection address so that it is effective? Do you think it would be useful beyond a Commonwealth agency audience?

g. What are your views on the proposal for the Commonwealth VC Trust Framework to be guidance-based rather than regulatory in nature? What limitations and trade-offs should the Government consider in making this choice?

h. What are the challenges that need to be overcome to achieve domestic and international interoperability of VCs and digital wallets, and how might they be overcome?

i. What sorts of behaviour needs to be guarded against or encouraged in a broader VC system?

j. How can VCs help to improve the inclusivity of government services? Are there any potential barriers to inclusion that VCs might inadvertently introduce?

k. Is the approach proposed for managing the complexities of a multi-standards environment for VCs fit-for-purpose (refer to Section 6.4 of this paper)? Do you consider there to be alternative approaches that the Government should also consider?

l. What challenges, risks, and potential drawbacks should the Government be aware of that may arise from the adoption of VCs by the Commonwealth and more broadly in Australia? How can these be mitigated?

Appendix A – Key concepts for VCs

Participants in a VC system

VCs function by interacting with four main participants: holders, issuers, verifiers, and trust services. A description of the role of each participant is described in the table, below.

Participant	Role
Holder	The subject of the credential, or an authorised representative for the subject of a credential, (for example, the parent of a child) who stores the VC in their digital wallet. The holder controls their data and chooses when and what information to share from a credential to others in face-to-face or online interactions.
Issuer	An authorised source that creates and provides the VC to holders. This could include Commonwealth, State and Territory Governments, as well as other private sector business and/or organisations, such as universities who provide educational qualifications.
Verifier	A business or organisation that needs to confirm something about an individual in order to provide a service, permit a transaction, or achieve another business outcome. The verifier examines VCs presented by a holder to confirm that the claims made are true and then undertakes subsequent business processes once the claim(s) are established (for example, continuing with the sale of age-restricted products).
Trust Service	A system that facilitates the technical verification of VCs, helping verifiers to decide whether they can trust a VC that is presented to them by a holder. There are various technical methods for building a trust service. Trust services are present in many, though not necessarily all, implementations of VCs.

Participants face several challenges including interoperability, security, trust, identity proofing and privacy. For issuers, one of the main challenges is to ensure the right person is issued the right credential, which necessitates strong identity proofing processes.

Verifiers (governments/businesses and other organisations) need to be able to trust that the credential presented is genuine and can be authenticated, so that they can provide a service, transaction or achieve a business outcome. This relies on secure systems and processes, and the implementation of suitable, interoperable trust services. Trust services for example, can provide a technical mechanism to perform cryptographic verification of a presented VC.

For holders, interoperability is a key challenges, alongside privacy. Acceptance of a VC wherever it is being used is key to unlocking its full suite of benefits, including user experience and adoption. The implementation of digital wallets plays a key role in addressing these challenges, as well as privacy preserving frameworks so that holders can control how they present and share their data, trust that their data is safe, and trust a verifier to handle their data appropriately once it has been shared.

The connections between the key players involved in creating and using VCs are demonstrated at a high level at Figure 1.

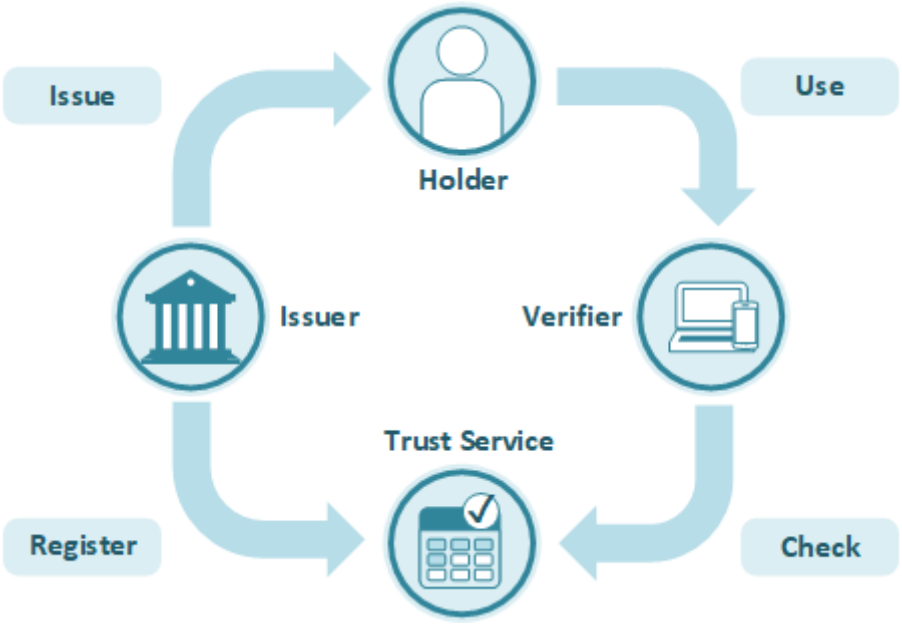

FIGURE 1: VERFIABLE CREDENTIALS – KEY ROLES

Lifecycle of a VC

The lifecycle of a VC typically encompasses the following stages.

- **Issuance**: the issuer creates the VC and digitally issues it to the holder's nominated device (often via a digital wallet).
- **Storage and use**: the holder stores the VC securely in their digital wallet (or other applicable device). The credential remains under the holder's control and they choose when and to whom to present it.
- **Reissuance and updates**: the credential can be updated as specific data fields change (such as the status of a licence) and/or reissued as needed throughout its active life. Depending on the nature of the credential and the circumstances, this action might be initiated by either the issuer or the holder.
- **Revocation**: the issuer may revoke a VC for various reasons, for example, if it was issued in error or the holder is no longer eligible for that VC. A VC might also be revoked on the expiration of a set time period.

Appendix B – Glossary

Term	Definition
Commonwealth VC Trust Framework	Should the Government develop a Commonwealth VC Trust Framework it is proposed to be a policy instrument that outlines tailored policy and technical settings and would be intended to guide standardised processes and practices for the adoption of VCs in Commonwealth agencies. The goals of the trust framework would include facilitating broad interoperability of VCs and ensuring that the people, businesses, and other organisations using VCs are properly protected. As guidance-based Commonwealth policy the trust framework would shape the decisions and delivery of Commonwealth agencies, while also providing sufficient flexibility so that the framework could be voluntarily adopted – in part or in whole – by other organisations if it proves useful.
Credential	A card, document, or other artefact issued by a trusted authority that serves as authoritative proof of relevant facts about a person or other legal entity. Credentials may be used to prove who we are (for example, proof of identity), something we are entitled to do (for example, licences), or a qualification we have achieved (for example, a university degree). Historically credentials have generally been available only in a physical form.
Cryptography	Cryptography enables securing of electronic messages using digital signatures and encryption. For VCs, encryption protects the credential's data and digital signatures provide assurance to the recipient that the credential has not been tampered with in transit.
Digital wallet	A software system hosted on a device controlled by an individual that offers functions that allow the individual to securely store, manage, and share their VCs. A digital wallet is privacy preserving and allows the individual to exercise their control to consent to present a VC for verification, selecting only the subset of data they wish to share with the verifier. Digital wallets are often used for other purposes alongside support for VCs, with a given digital wallet potentially offering functions such as storage for digital copies of documents/cards, operating digital authenticators, and facilitating digital payments (the latter is understood to be the most prevalent of all use cases for digital wallets).
Holder	The subject of the credential, or an authorised representative for the subject of a credential, (for example, the parent of a child) who stores the VC in their digital wallet. The holder controls their data and chooses when and what information to share from a credential to others in face-to-face or online interactions.

Term	Definition
Interoperability	Interoperability for VCs refers to the capability for different systems, organisations and jurisdictions to recognise, exchange, and accept the presentation of credentials seamlessly regardless of the issuing platform, whilst maintaining security, trust and privacy. Interoperability across many and varied participants is driven by the adoption of standards. Achieving interoperability between the issuer, holder, and verifier systems in a VC network allows people to present and reuse their credentials with a wide range of participants in a broad set of use cases.
Issuer	An entity that is the source of truth for information contained in a VC. On request they create and issue VCs to holders. This could include Commonwealth, State and Territory Governments, as well as other private sector business and/or organisations, such as universities who provide educational qualifications.
Standards	Standards are agreed technical specifications that describe how to implement a particular solution and may outline rules, requirements, and other guidance to achieve technical compatibility. For VCs, there are understood to be several different standards-based approaches available in the community, with each offering different features and strengths. In many cases a group of complementary standards will need to be followed to implement a holistic VC solution. Standards are developed and published by standards setting organisations. For example, VC standards have been published by organisations including the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), the World Wide Web Consortium (W3C), and the Internet Engineering Task Force (IETF).
Trust service	A system that facilitates the technical verification of VCs, helping verifiers to decide whether they can trust a VC that is presented to them by a holder. There are various technical methods for implementing a trust service. Trust services are present in many, though not necessarily all, implementations of VCs.
Use case	A particular scenario or instance where VCs are used in place of traditional credentials. For example, the presentation of a Medicare VC to register at a medical clinic (instead of using a plastic Medicare card) is a VC use case.
VC	Abbreviation for ‘verifiable credential’.

Term	Definition
Verifiable credential (VC)	A digital representation of a traditional credential (for example, a driver licence, Medicare card, or proof of an educational qualification) that is stored on your device and can be independently verified through cryptographic methods. With the consent of the individual, the VC can be presented to a third party to prove that the credential is genuine. Defining characteristics of a VC generally include: • an architectural pattern with issuer, holder and verifier as primary actors • dedicated trust mechanisms to allow independent verification of authenticity • selective control by the holder of what subset of credential data is shared with verifiers, and • being cryptographically secure and tamper evident. A VC can be verified with the appropriate software without needing to contact the issuer of the credential. VCs can be reissued, updated, and revoked. A VC is not simply a digital copy or image of a physical credential stored on a device, nor is the definition of a VC limited to compliance with any particular implementation standard.
Verifier	A business or organisation that needs to confirm something about an individual in order to provide a service, permit a transaction, or achieve another business outcome. The verifier examines VCs presented by a holder to confirm that the claims made are true and then undertakes subsequent business processes once the claim(s) are established (for example, continuing with the sale of age-restricted products once a VC has been used to verify that the customer is over 18 years old).